Exhibit C

Crypto Thieves Get Bolder by the Heist, Stealing Record Amounts

WSJ wsj.com/articles/crypto-thieves-get-bolder-by-the-heist-stealing-record-amounts-11650582598

April 22, 2022

Cryptocurrency hacks are getting bigger.

On Sunday, a hacker exploited a new algorithmic stablecoin project called Beanstalk and drained it of $182 million worth of digital assets.

The hack wiped out all of the ether held by the fund. Once the ether was removed, the value of the stablecoin itself, called Bean, collapsed to 10 cents from $1 on Sunday, according to data firm CoinGecko. Most recently it was trading at 6 cents.

After the bean stablecoin's collapse, the hacker's profit was about $76 million, according to a blog post from Beanstalk Farms, the group that operates the project.

The Beanstalk hack was the fifth-largest crypto theft on record, according to Rekt.news, which tracks crypto hacks. The hack follows a $540 million theft last month from the platform for the online game Axie Infinity.

The 2022 pace of roughly a hack a week is in line with last year, but the amount stolen is rising, according to Rekt. Since August, there have been 37 hacks in 38 weeks that have drained about $2.9 billion worth of cryptocurrencies.

That is on par with the $3.2 billion stolen in all of 2021, according to analytics firm Chainalysis.

Hackers are finding larger exploits amid the increase of decentralized finance, or DeFi, projects. Hackers tend to target new protocols that haven't been fully tested and vetted, said Max Galka, chief executive of crypto forensics firm Elementus.

Beanstalk just launched in August.

The open-source nature of DeFi projects is another reason they are attractive to thieves. Hackers can spend time examining the code looking for weaknesses, Chainalysis said. Even platforms that have audited their code have still been hacked. The firm said DeFi protocols need to have a more thorough approach to security.

Most of the hacks have taken advantage of faulty code, according to Chainalysis. In fact, the exact method that the Beanstalk hacker used has become a common one, the firm said.

The Beanstalk protocol used what's called a DAO, or decentralized autonomous organization. Users can dedicate, or "stake," funds to the project, which gives them a vote in governance and changes to the protocol.

According to blockchain-analytics firm Elliptic, the hacker borrowed about $1 billion worth of different stablecoins, using an ultra-short-term kind of loan called a flashloan, and then added that to Beanstalk's funds. That was enough to give them an overwhelming percentage of voting power.

The hacker proposed donating money to Ukraine, and voted to approve the idea. The proposal, however, included code that instead sent all the funds locked up in the Beanstalk protocol to a wallet controlled by the hacker, according to Elliptic.

Once they stole the funds, they repaid the loan, and pocketed the difference.

Bitcoin's volatility has limited its adoption for payments, so entrepreneurs created stablecoins: cryptocurrencies pegged to assets such as the U.S. dollar. But the recent settlement of a probe into the most popular stablecoin, tether, shows the need for transparency in the growing industry. Photo illustration: Sharon Shi/WSJ

Ironically, Mr. Galka pointed out, the hacker was following Beanstalk's stated rules. The problem is there was no contingency for somebody taking over the voting mechanism, which reflects the newness of the project itself, he said.

"Everything this guy did was consistent with the code," Mr. Galka said.

Publius, the development group that launched Beanstalk, declined to comment for this article.

The developer group has been trying to regroup and has said it wants to attempt to rebuild. To do so would require securing the protocol, finding new capital to fund it, as well as repaying users who lost money from the hack.

It is unclear if any of the funds can be recovered. The developers behind Beanstalk asked the hacker to return the funds but keep 10% as a "bug bounty." So far there has been no reply to that request.

Write to Paul Vigna at Paul.Vigna@wsj.com

Appeared in the April 23, 2022, print edition as 'Hackers Get Bolder In Crypto Capers'.